
ORACLE®

JavaOne™

ORACLE®

Keep Learning with Oracle University

ORACLE UNIVERSITY

Classroom Training

Learning Subscription

Live Virtual Class

Training On Demand

Cloud

Technology

Applications

Industries

education.oracle.com

Session Surveys

Help us help you!!

- Oracle would like to invite you to take a moment to give us your session feedback. Your feedback will help us to improve your conference.
- Please be sure to add your feedback for your attended sessions by using the Mobile Survey or in Schedule Builder.

How Would *You* Improve the Java EE Security API?

JSR 375

Ivar Grimstad, Expert Group Member
Alex Kosowski, Spec Lead
October 27, 2015

JavaOne
ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Program Agenda

1. Ideas
2. Demo
3. Get Involved
4. What do you think?

Program Agenda

1. Ideas
2. Demo
3. Get Involved
4. What do you think?

Java EE Security API 1.0

JSR 375

- Improve portability, modernize, simplify
- Incorporate CDI, Expression Language, Lambda Expressions
- Terminology
- API for Authentication Mechanism
  - Simplify JASPIC authentication module development and usage
  - CDI Events: PreAuthenticate, PostAuthenticate, PreLogout, PostLogout
- API for Identity Store
  - CDI bean for validating credentials and accessing group and role mapping
  - JAAS adapter for potentially leveraging existing LoginModules

Java EE Security API 1.0

JSR 375

- API for Password Aliasing
  - Standard syntax/rules for password alias usage in annotations and deployment descriptors
- API for Role/Permission Assignment
  - Application portable group to role mapping
  - One-to-one group to role mapping
  - Application changeable role mapping, to dynamically upgrade/downgrade privilege

Java EE Security API 1.0

JSR 375

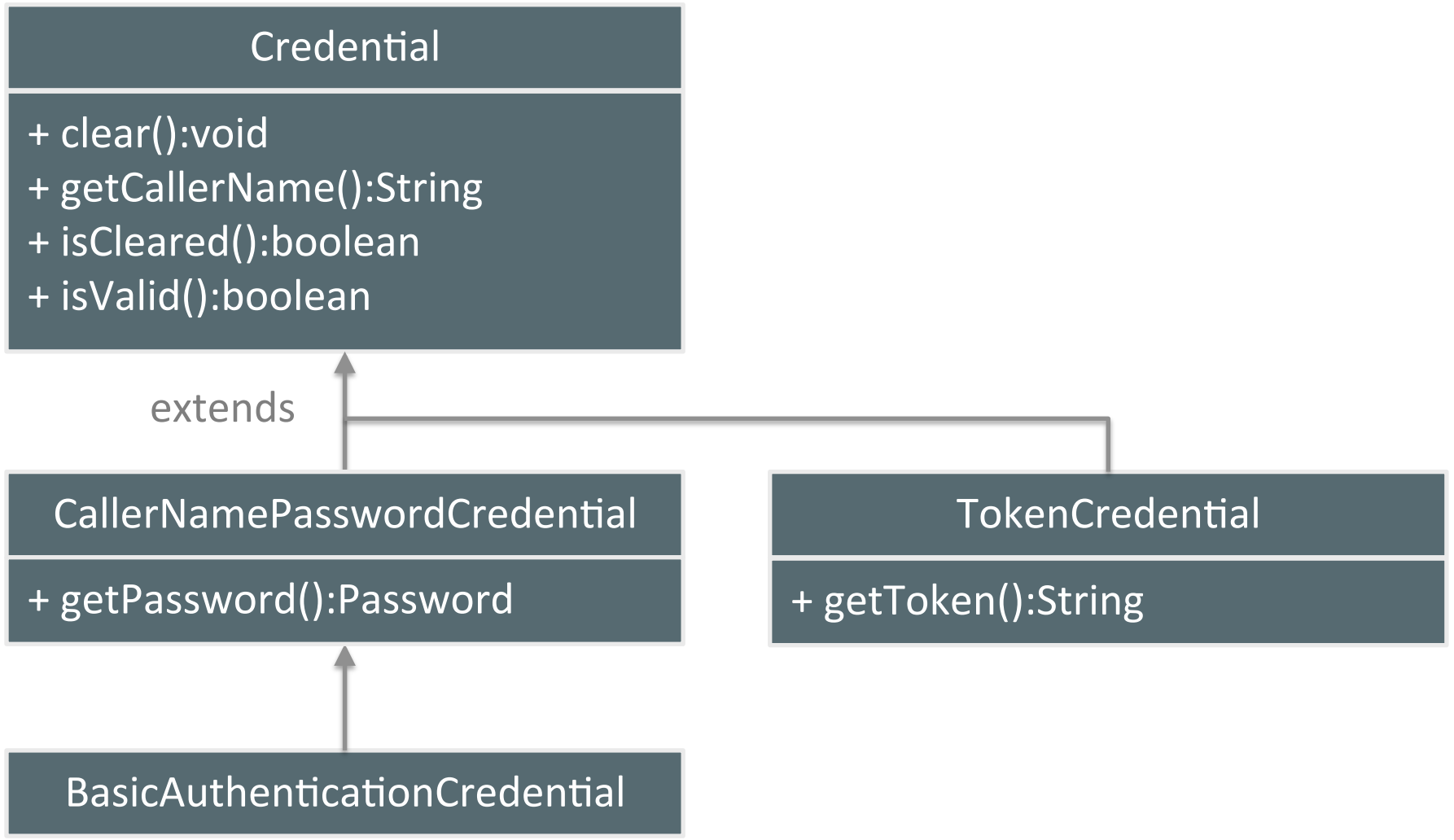
- API for Security Context
  - CDI bean for accessing Security Context, uniform API in all containers
  - login(), logout(), runAs(), isAuthenticated(), isUserInRole()
  - For all managed beans: CDI, Servlet, EJB, JAX-RS, etc
- API for Authorization Interceptors
  - Expression Language Authorization Rules
  - AccessDecisionVoter

Program Agenda

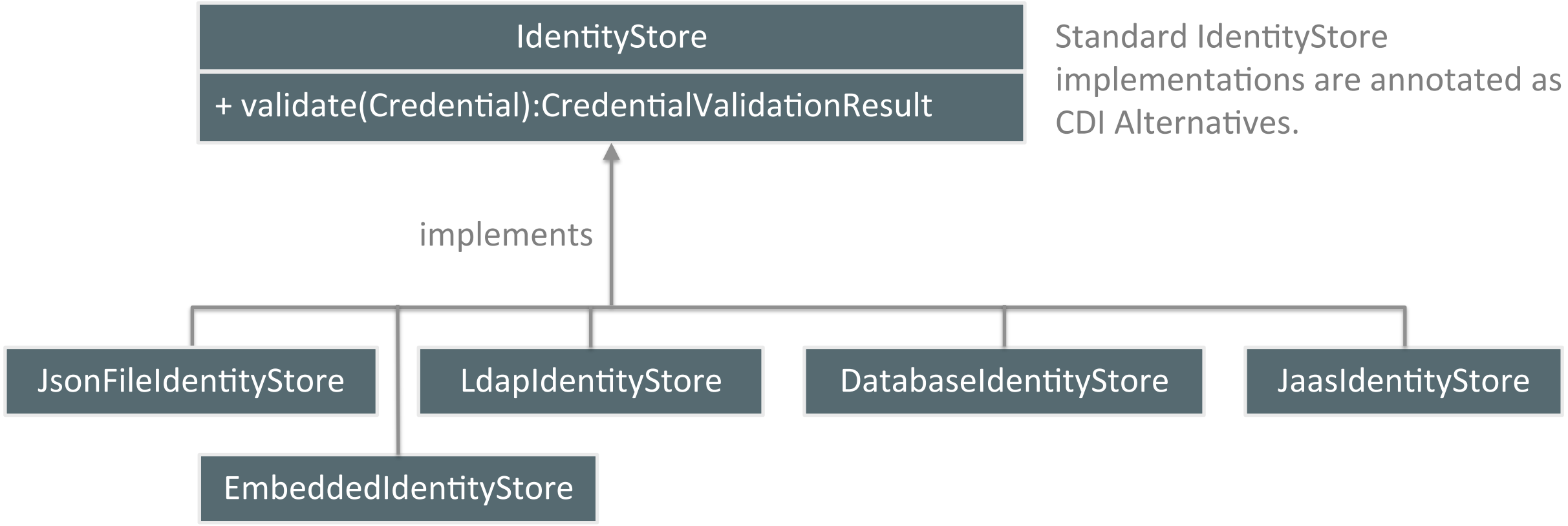
1. Ideas
2. Demo
3. Get Involved
4. What do you think?

Ideas – Identity Store Interaction

Ideas – Identity Store Credentials



Ideas – Identity Store Standard Implementations



Standard IdentityStore implementations are annotated as CDI Alternatives.

Demo – JASPIC SAM using EmbeddedIdentityStore

- BIG thank you to Arjan Tijms for developing the demo!
- Go to demo…

Program Agenda

1. Ideas
2. Demo
3. **Get Involved**
4. What do you think?

Get Involved

Contribute to the JSR!

- Project Page: The starting point to all resources
  https://java.net/projects/javaee-security-spec

- Users List: Subscribe and contribute
  users@javaee-security-spec.java.net

- Github Playground: Fork and Play!
  https://github.com/javaee-security-spec/javaee-security-proposals

Project Features
- Downloads
- Issue Tracking
- Mailing Lists
- Source Code Repositories
  - Miscellaneous
  - Spec-API
- API JavaDoc
- WikiHomePage
- Java EE Security API Spec

Project Links
- Github Playground
- Google Group Folder
- Upcoming Events
- JSR-375 JCP Page

About this Project

Java EE Security API Specification was started in November 2014 and has 33 members. The project administrators are Ed Bratt and alex.kosowski.

Join This Project

Last updated 2 minutes ago, by alex.kosowski

Java EE Security API Specification 1.0

Please share your ideas by joining the users list.

This is the project for the Java EE Security API specification. The goal of this specification is to improve the Java EE platform by ensuring the Security API aspect is useful in the modern cloud/PaaS application paradigm. This promotes self-contained application portability across all Java EE servers, and promotes use of modern programming concepts such as expression language, and contexts and dependency injection. This specification will holistically attempt to simplify, standardize, and modernize the Security API across the platform in areas identified by the community.

The Java EE Security API specification is on the JCP Ballot as JSR 375, for inclusion in Java EE 8.

Current Stage: *Early Draft Development*

Epics

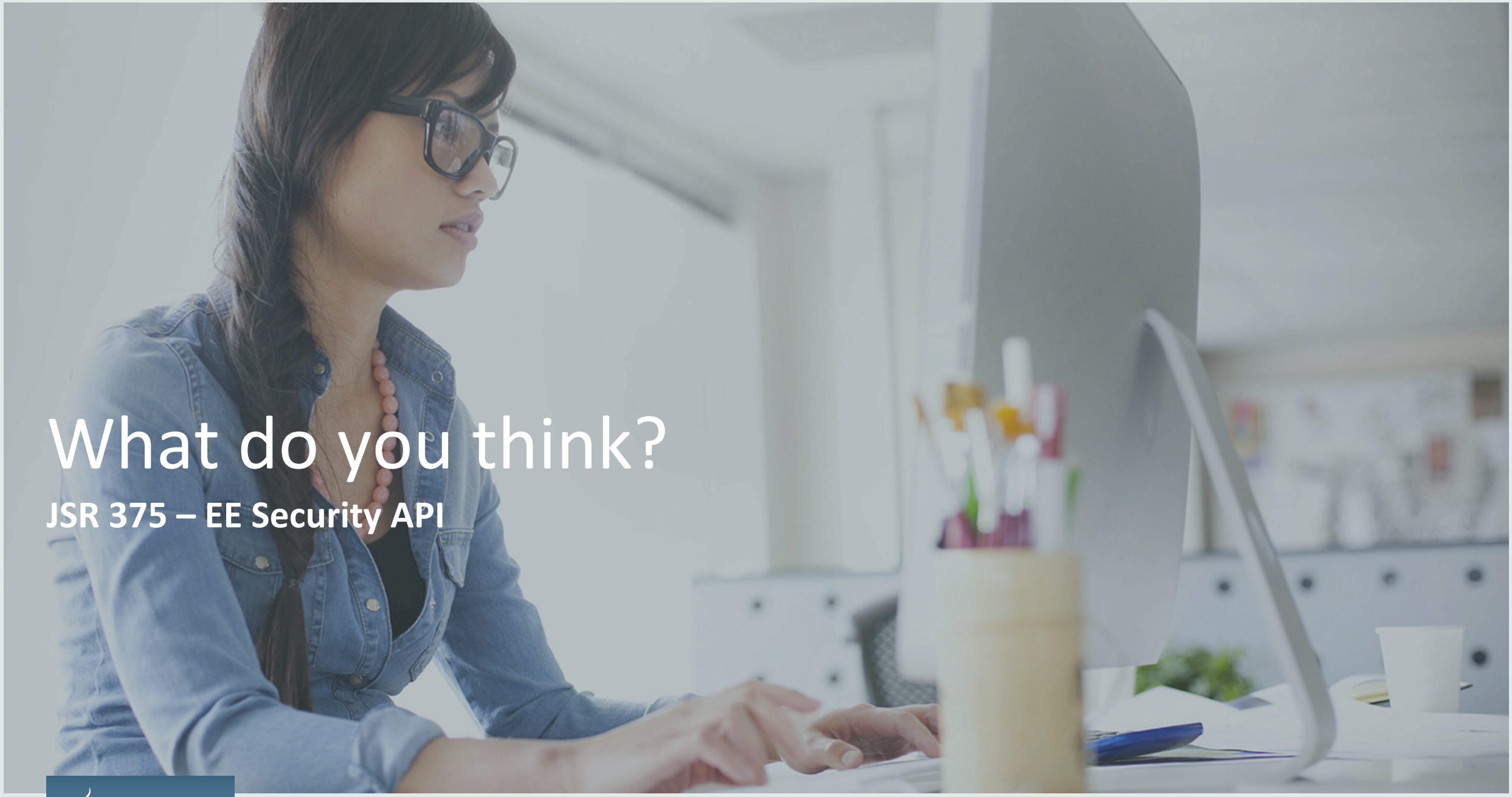
Name	Status	Links	Description
Terminology	In Progress	epic proposal	Establish Security API terminology to enable accurate and concise communication
Authentication Mechanism	In Progress	epic	Simplify application-accessible authentication mechanisms
Identity Store	In Progress	epic proposal poc javadoc	Standardize application-accessible identity store
Role/Permission Assignment	Not Started		Standardize application-accessible role/permission assignment
Security Context	Not Started		Standardize a platform-wide Security Context
Authorization Interceptors	Not Started		Standardize platform-wide Authorization Interceptors
Password Aliasing	Not Started		Standardize the API for using password aliases in configuration
Standardized Server Authentication Modules	Not Started		Using the simplified Authentication Mechanism, standardize some additional ServerAuthModules

Links:

- epic = Link to JIRA Epic, which is a collection of issues
- javadoc = Link to related JavaDoc
- poc = Link to proof of concept code
- proposal = Link to proposal document
- spec = Link to specification text

Program Agenda

1. Ideas
2. Demo
3. Get Involved
4. What do you think?



What do you think?

JSR 375 – EE Security API

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Integrated Cloud

Applications & Platform Services

JavaOne™

ORACLE®


ORACLE®